UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/791,160	03/01/2004	Mitchell B. Oliver	020294	3432

23696 7590 10/07/2009
QUALCOMM INCORPORATED
5775 MOREHOUSE DR.
SAN DIEGO, CA 92121

EXAMINER	
PATEL, DHAIRYA A	
ART UNIT	**PAPER NUMBER**
2451	
NOTIFICATION DATE	**DELIVERY MODE**
10/07/2009	ELECTRONIC

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Notice of the Office communication was sent electronically on above-indicated "Notification Date" to the following e-mail address(es):

us-docketing@qualcomm.com
kascanla@qualcomm.com
nanm@qualcomm.com

Office Action Summary	**Application No.** 10/791,160	**Applicant(s)** OLIVER ET AL.	
	Examiner Dhairya A. Patel	**Art Unit** 2451	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *24 March 2009*.

2a)☒ This action is **FINAL**. 2b)□ This action is non-final.

3)□ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-24* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)□ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-24* is/are rejected.

7)□ Claim(s) _____ is/are objected to.

8)□ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)□ The specification is objected to by the Examiner.

10)□ The drawing(s) filed on _____ is/are: a)□ accepted or b)□ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)□ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)□ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)□ All b)□ Some * c)□ None of:

1.□ Certified copies of the priority documents have been received.

2.□ Certified copies of the priority documents have been received in Application No. _____.

3.□ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)

2) □ Notice of Draftsperson's Patent Drawing Review (PTO-948)

3) ☒ Information Disclosure Statement(s) (PTO/SB/08)
Paper No(s)/Mail Date _____.

4) □ Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____ .

5) □ Notice of Informal Patent Application

6) □ Other: _____.

DETAILED ACTION

1. This action is responsive to communication filed on 3/24/2009. Claims 1-24 are subject to examination. Claims 22-24 are newly added claims.

Information Disclosure Statement

The information disclosure statement (IDS) submitted on 3/24/2009 is in compliance with the provisions of 37 CFR 1.97. Accordingly, the information disclosure statement is being considered by the examiner.

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

Claims 1-10,22-24 are rejected under 35 U.S.C. 103(a) as being unpatentable over Shenfield et al. U.S. Patent Publication # 2004/0220998 (hereinafter Shenfield) in view of Kiiveri et al. U.S. Patent Publication # 2005/0033969 (hereinafter Kiiveri)

As per claim 1, Shenfield teaches a computer device (having wireless communication capability, comprising:

-a wireless communication portal for selectively sending and receiving data across a wireless network (Paragraph 23); **NOTE:** The reference teaches transmitting and receiving requests/response message in the form of message header information and associated data content for example product pricing and availability etc across wireless network.

-a computer platform including a resident application environment and selectively download applications to the platform through the portal, the resident application environment configured to selectively download application that comply with a predefined security protocol (Paragraph 24)(Paragraph 58); **NOTE:** The reference teaches downloading client application program in relation to the application server (a computer platform). The presentation components program and workflow program (resident application environment) in the application server using username and password (utilizing a predefined security protocol). If the login is correct the specials screen is displayed i.e. presentation components (downloading an application).

-a data store (i.e. storage module in memory) in communication with the computer platform and selectively sending data to and receiving data from the computer platform (Paragraph 33, 34, 58, 59, 64); and

Shenfield is silent in teaching a download manager resident on the computer platform that at least selectively downloads applications that do not comply with the predefined security protocol.

Kiiveri teaches a download manager resident on the computer platform that at least selectively downloads applications that do not comply with the predefined security protocol (Paragraphs 29, 32) **NOTE:** The reference teaches if signature check fails (do not comply with the predefined security protocol), unsecured mode is activated and the non-verified application is loaded in ASIC RAM (downloading applications that do not comply) located outside the secure environment.

Kiiveri also teaches a computer platform (i.e. ASIC) including a resident application (boot application) environment and selectively download application that comply with a predefined security protocol (Paragraph 24,25);**NOTE:** The reference teaches ASIC (i.e. computer platform) including a boot application (resident application) environment for selectively downloading new application, the boot application utilizing secured environment software to control the download and execution.

-a data store in communication with the computer platform and selectively sending data to and receiving data from the computer platform (Paragraph 31) (claim 1 limitation ”storage circuit”). It would have been obvious to one of ordinary skill in the art at the time of applicant’s invention was made to implement Kiiveri’s teaching in Shenfield’s teaching to come up with having downloading application that does not comply with security protocol. The motivation for doing so would be so that testing, debugging and servicing the mobile telecommunication terminal and its software without risking that a third party is given access to information which makes it possible to manipulate the security related components of the device so as to affect the security functions (paragraph 29).

As per claim 2, Shenfield and Kiiveri teaches the device of claim 1, but Kiiveri further teaches wherein the download manager exists within resident application environment and uses an existing application download interface (Paragraph 32).

As per claim 3, Shenfield and Kiiveri teaches the device of claim 1, but Kiiveri further teaches wherein the downloaded application is immediately executed (Paragraph 32).

As per claim 4, Shenfield and Kiiveri teaches the device of claim 1, but Kiiveri further teaches wherein a downloaded application that does not comply with the predefined security protocol is stored, and the stored application is executed through the download manager (Paragraph 29,32).

As per claim 5, Shenfield and Kiiveri teaches the device of claim 1, but Kiiveri further teaches wherein the download manager further manages executing the downloaded application that does not comply with the predefined security protocol (Paragraph 28,29,32).

As per claim 6, Kiiveri teaches the device of claim 4, wherein the download manager further manages storage of the downloaded application that does not comply with the predefined security protocol in the data store (Paragraph 29, 32).

As per claim 7, Shenfield and Kiiveri teaches the device of claim 1, but Kiiveri further teaches wherein the predefined security protocol is verifying the origination of the application (Paragraph 27).

As per claim 8, Shenfield and Kiiveri teaches the device of claim 1, but Kiiveri further teaches wherein the predefined security protocol is verifying the presence of a certificate within the downloaded application (Paragraph 27, 30).

As per claim 9, Kiiveri teaches the device of claim 5, wherein the download manager executes the downloaded application that does not comply with the predefined security protocol outside of the resident application environment (Paragraph 28, 29, 32). **NOTE:** The reference clearly states RAM which stores the non-verified software is executed by CPU outside the secure environment.

As per claim 10, Shenfield teaches a computer device having wireless communication capability, comprising: a wireless communication means for selectively sending and receiving data across a wireless network (Paragraph 23); **NOTE:** The reference teaches transmitting and receiving requests/response message in the form of message header information and associated data content for example product pricing and availability etc across wireless network.

a computer means selectively downloading applications through the wireless communication means, the computer means configured to selectively download application that comply with a predefined security protocol (Paragraph 24)(Paragraph 58); **NOTE:** The reference teaches downloading client application program in relation to the application server The presentation components program and workflow program (resident application environment) in the application server using username and password (utilizing a predefined security protocol). If the login is correct the specials screen is displayed i.e. presentation components (downloading an application).

Shenfield is silent in teaching a means for selectively downloading applications that do not comply with the predefined security protocol.

Kiiveri teaches a means for selectively downloading applications that do not comply with the predefined security protocol (Paragraphs 29, 32) **NOTE:** The reference teaches if signature check fails (do not comply with the predefined security protocol), unsecured mode is activated and the non-verified application is loaded in ASIC RAM (downloading applications that do not comply) located outside the secure environment.

Kiiveri also teaches a computer means selectively downloading applications through the wireless communication means, configured to selectively download application that comply with a predefined security protocol (Paragraph 24); **NOTE:** The reference teaches ASIC (i.e. computer platform) including a boot application (resident application) environment for selectively downloading new application, the boot application utilizing secured environment software to control the download and execution.

It would have been obvious to one of ordinary skill in the art at the time of applicant's invention was made to implement Kiiveri's teaching in Shenfield's teaching to come up with having downloading application that does not comply with security protocol. The motivation for doing so would be so that testing, debugging and servicing the mobile telecommunication terminal and its software without risking that a third party is given access to information which makes it possible to manipulate the security related components of the device so as to affect the security functions (paragraph 29).

As per claim 22, Kiiveri teaches the computer device of claim 1, wherein the download manager exists within resident application environment and uses an existing application download interface (Paragraph 24), and wherein the download manager further manages executing the downloaded application that does not comply with predefined security protocol (Paragraph 28-29).

As per claim 23, Kiiveri teaches the computer device of claim 1, wherein the pre-defined security protocol includes an application validation requirement of the resident application environment (Paragraph 27,30,31). **NOTE:** The reference teaches having signature verification of the downloaded software fails i.e. checksums does not match or the operation of the ASIC which is checked (validation requirement) by the secure environment software (resident application environment)

As per claim 24, Kiiveri teaches the computer device of claim 1, wherein the application being downloaded by the resident application environment in compliance with the pre-defined security protocol and the application being downloaded by the download manager in non-compliance with the pre-defined security protocol are both stored in the data store (Paragraph 28, 29, 32).

Claim Rejections - 35 USC § 102

The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (e) the invention was described in a patent granted on an application for patent by another filed in the United States before the invention thereof by the applicant for patent, or on an international application by another who has fulfilled the requirements of paragraphs (1), (2), and (4) of section 371(c) of this title before the invention thereof by the applicant for patent.

The changes made to 35 U.S.C. 102(e) by the American Inventors Protection Act of 1999 (AIPA) and the Intellectual Property and High Technology Technical Amendments Act of 2002 do not apply when the reference is a U.S. patent resulting directly or indirectly from an international application filed before November 29, 2000.

Therefore, the prior art date of the reference is determined under 35 U.S.C. 102(e) prior to the amendment by the AIPA (pre-AIPA 35 U.S.C. 102(e)).

Claims 11-21 are rejected under 35 U.S.C. 102(e) as being anticipated by Kiiveri et al. U.S. Patent Publication # 2005/0033969 (hereinafter Kiiveri)

As per claim 11, Kiiveri teaches a method of selectively downloading through a wireless connection to a computer device an application that does not comply with a predefined security protocol for use at that computer device, comprising the steps of: downloading to a computer platform (i.e. ASIC) of the computer device an application that does not comply with a predefined security protocol for use at that computer device (Paragraphs 29, 32) **NOTE:** The reference teaches if signature check fails (do not comply with the predefined security protocol), unsecured mode is activated and the non-verified application is loaded in ASIC RAM (downloading applications that do not comply) located outside the secure environment.

-the computer platform including a resident application environment for downloading and executing applications utilizing a predefined security protocol for at least downloading an application, the downloading of the non-complying application occurring through the use of a download manager resident on the computer platform; (Paragraph 24);**NOTE:** The reference teaches ASIC (i.e. computer platform) including a boot application (resident application) environment for selectively downloading new application, the boot application utilizing secured environment software to control the download and execution.

-executing the application at the computer device with the download manager (paragraph 32).

As per claim 12, Kiiveri teaches the method of claim 11, wherein the download manager exists within resident application environment and the step of downloading uses an existing application download interface (Paragraph 32).

As per claim 13, Kiiveri teaches the method of claim 11, further comprising the steps of: storing, with the download manager (claim 1 limitation “storage circuit”) (Paragraph 28), the downloaded application that does not comply with the predefined security protocol (Paragraph 28); and executing the stored application through the download manager (paragraph 28) (Paragraph 32).

As per claim 14, Kiiveri teaches the method of claim 11, further comprising the step of verifying the nature of the downloaded application as the predefined security protocol (Paragraph 27).

As per claim 15, Kiiveri teaches the method of claim 14, wherein the step of verifying the nature of the downloaded application is verifying the presence of a certificate within the downloaded application (Paragraph 27, 30).

As per claim 16, Kiiveri teaches the method of claim 11, wherein the step of executing the downloaded application with the download manager occurs outside of the resident application environment (Paragraph 28, 32).

As per claim 17, Kiiveri teaches the method of claim 11, further comprising the step of downloading the download manager to the computer platform of the computer device after a request to download an application that does not comply with a predefined security protocol has been made, and prior to the step of downloading the requested application (Paragraph 32).

As per claim 18, Kiiveri teaches a method of selectively downloading through a wireless connection to a computer device an application that does not comply with a predefined security protocol for use at that computer device, comprising the steps of: a step for downloading to a computer platform of the computer device an application that does not comply with a predefined security protocol for use within a resident application environment at that computer device (Paragraphs 29, 32) **NOTE:** The reference teaches if signature check fails (do not comply with the predefined security protocol), unsecured mode is activated and the non-verified application is loaded in ASIC RAM (downloading applications that do not comply) located outside the secure environment.

-a step for executing the downloaded application at the computer device outside of the resident application environment (Paragraph 28, 29, 32). **NOTE:** The reference clearly states RAM which stores the non-verified software is executed by CPU outside the secure environment.

As per claim 19, it teaches same limitation as claim 11, therefore rejected under same basis.

As per claim 20, Kiiveri teaches the program of claim 19, wherein the download manager is resident on the computer platform (Paragraph 32). **NOTE:** The reference teaches RAM is resident of ASIC (computer platform).

As per claim 21, Kiiveri teaches the program of claim 19, wherein the download manager is loaded to the computer platform after a request to download of an application that does not comply with a predefined security protocol and prior to download thereof (Paragraph 32). **NOTE:** The reference teaches non-verified application is loaded into ASIC RAM located outside the secure environment after the signature check fails (does not comply with a predefined security).

Response to Arguments

Applicant's arguments filed 3/24/2009 have been fully considered but they are not persuasive.

A). Applicant states Shenfield does not “computer devices having wireless communication capability” and that computer devices in Shenfield is more generic ”computer device”.

As per remark A, Examiner respectfully disagrees with the applicant because in Fig. 1 element 100 which are computer devices are shown as mobile phone and pager and are connected to a wireless network. Since the computer devices are connected to wireless network, it means they have wireless communication capability. Also in Paragraph 23, Shenfield specifically states system 10 comprises mobile communication devices (Fig. 1 element 100) coupled via wireless network. Therefore Shenfield reads on the claimed limitations.

B). Applicant states Kiivera does not disclose or suggest “the resident application environment configured to selectively download applications that comply with a predefined security protocol” and “a download manager resident on the computer platform that is configured to selectively downloads application that do not comply with the pre-defined security protocol". Applicant also states that Kiiveri does not disclose or suggest the mechanism responsible for downloading the non-verified application is also responsible for its execution

As per remark B, Examiner respectfuly disagrees with the applicant in Paragraph 24, Kiiveri teaches a computer platform (i.e. ASIC) including a resident application (boot application) environment and selectively downloading applications to the platform through the portal, the resident application environment utilizing a predefined security protocol for at least downloading an application (Paragraph 24). Kiiveri further teaches ASIC (i.e. computer platform) including a boot application (resident application) environment for selectively downloading new application, the boot application utilizing secured environment software to control the download and execution. Kiiveri specifically states new protected application can be downloaded into the secure environment. Kiiveri also states secure environment software controls the download and execution of protected application and only signed protected application are allowed to run which means secure environment software (i.e. resident application) configured to download only protected application which comply with secure environment (predefined security protocol).

In Paragraph 29, 32, Kiiveri teaches a download manager resident on the computer platform that at least selectively downloads applications that do not comply with the predefined security protocol (Paragraphs 29, 32). Kiiveri further teaches if signature check fails (do not comply with the predefined security protocol), unsecured mode is activated and the non-verified application is loaded in ASIC RAM (downloading applications that do not comply) located outside the secure environment.

Examiner would like to point out that in Paragraph 28, Kiiveri teaches that a RAM is arranged outside of secure environment in the ASIC, which RAM holds the non-verified software executed by the CPU. This means that non-verified software i.e. non-complying application is downloaded by ASIC in RAM which is then executed by the CPU. Therefore this means the CPU is responsible for executing the non-verified software which is stored in RAM and downloaded by ASIC in RAM, therefore Kiiveri reads the claimed limitations.

Therefore Kiiveri teaches the claimed limitations.

C). Applicant states Kiivera would not be possible to execute the download manager and/or execution of the downloaded application via the download manager during secure mode.

As per remark C, Examiner respectfully disagrees with the applicant because in Paragraph 28-29, Kiiveri teaches that RAM holds the non-verified software and is executed by the CPU. Claim language of claim 22, states “download manager exists within resident application environment and uses an existing application download interface and wherein the download manager further manages executing the downloaded application that does not comply with predefined security protocol”. Claim language does not state " to execute the download manager and/or execution of the downloaded application via the download manager during secure mode.” Furthermore, CPU exists during the secure environment/non-secure environment which it uses non-secure environment software to download the non-verified software and CPU is executing the non-verified software. Therefore Kiivera reads on the claimed limitations and claim language does not state " to execute the download manager and/or execution of the downloaded application via the download manager during secure mode."

Conclusion

2. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

   A). Kiessling et al. U.S. Patent # 6,901,251

   B). Stillerman et al. U.S. patent # 7,467,417/

3. A shortened statutory period for response to this action is set to expire **3 (three) months and 0 (zero) days** from the mail date of this letter. Failure to respond within the period for response will result in **ABANDONMENT** of the applicant (see 35 U.S.C 133, M.P.E.P 710.02, 710.02(b)).

THIS ACTION IS MADE FINAL. Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of this final action.

4.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Dhairya A. Patel whose telephone number is 571-272-5809. The examiner can normally be reached on Monday-Friday 8:00AM-5: 30PM, first Fridays OFF.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, John Follansbee can be reached on 571-272-3964. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

DAP

/John Follansbee/
Supervisory Patent Examiner, Art Unit 2451